

REMARKS/ARGUMENTS

Claims 1-17 are pending in the present application, of which claims 1 and 11 are independent. Claims 1, 2, 8, 11, and 16 are amended.

The courtesies extended to Applicant's representative by Examiner of Record Trong Nguyen and Supervisory Primary Examiner Nasser Moazzami at the interview held on May 13, 2009, are appreciated. The reasons presented at the interview as warranting favorable action are incorporated into the remarks below and constitute Applicant's record of the interview.

CLAIM OBJECTIONS

On pages 3-4, the Office Action objects to claims 1, 8, 11, and 16. Applicant respectfully traverses these objections and addresses each item separately.

For claim 1, the Office Action alleges that "further" should be omitted. In response, Applicant adopts the Examiner's suggestion.

For claim 8, the Office Action alleges that "is adapted to perform" does not limit the scope of the claim. In response, Applicant hereby replaces the cited language with the verb "performs."

For claim 11, the Office Action alleges that "the calculated key" should be amended to "the calculated round key" and that "the transferred key" should be

amended to “the transferred round key.” In response, Applicant amends the cited language to “the at least one round key” for consistency with the antecedent.

For claim 11, the Office Action further alleges that “using” should be omitted. In response, Applicant adopts the Examiner's suggestion.

For claim 16, the Office Action alleges that “the data” should be changed to “the external data.” In response, Applicant adopts the Examiner's suggestion.

Having addressed all of the objections as described above, Applicant respectfully requests withdrawal of the objections to claims 1, 8, 11, and 16.

REJECTIONS UNDER 35 U.S.C. § 103

1. Independent Claims 1 and 11, Dependent Claims 4, 8, 9, 15, and 16

On pages 4-11, the Office Action rejects claims 1, 4, 8, 9, 11, 15, and 16 under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent No. 5,261,003 to Matsui (hereinafter “Matsui”) in view of U.S. Patent Application No. 2002/0021802 to Muratani (hereinafter “Muratani”). Applicant respectfully traverses this rejection.

Independent claim 1 now recites, in part, the following subject matter “a first request line that sends requests from the at least one encryption/decryption device to the control device; and a second request line that sends requests from the round key generator to the control device, wherein the at least one

encryption/decryption device and the round key generator both transmit requests on the respective first and second request lines to start the encryption/decryption operation **after both requests are met**" (emphasis added). Independent claim 11 contains a similar recitation. This subject matter finds support in the specification in, for example, paragraph [0032] of the published version of the Specification. This use of request lines provides increased safety against attacks because there is no longer a direct data path between the at least one encryption/decryption device and the round key generator, as further disclosed in paragraph [0004].

Applicant respectfully submits that Matsui and Muratani, alone or in combination, do not disclose, teach, or suggest this subject matter. As discussed during the Interview on May 13, 2009, the references of record do not start an encryption/decryption operation after waiting for both requests to be met. Applicant addresses aspects of both references individually below.

Matsui provides for only a single input terminal (Fig. 1: 3) for acquisition of plain text. Thus, Matsui lacks the separate provision of an initial key to the control device. Therefore, Matsui teaches away from having separate request lines for encryption/decryption and round key generation. Instead, Matsui directly couples encryption/decryption and "extended key" sections, having no need of separate requests to an intervening control device. Moreover, Matsui cannot provide a wait period before starting an encryption/decryption operation.

Muratani has similar deficiencies. As shown in Fig. 1, Muratani's data randomizing section is directly coupled to the expanded key scheduling section. While Muratani has separate lines for "plaintext" and "common key," Muratani teaches away from the use of separate request lines because Muratani lacks an intervening control device coupled to first and second request lines.

Thus, claims 1 and 11 are allowable over Matsui in view of Muratani. Claims 4, 8, and 9 depend from claim 1. Claims 15 and 16 depend from claim 11. Thus, claims 4, 8, 9, 15, and 16 are allowable at least due to their respective dependencies from allowable claims. Therefore, Applicant respectfully requests withdrawal of the rejection of claims 1, 4, 8, 9, 11, 15, and 16 under 35 U.S.C. § 103(a).

2. Dependent Claims 2 and 3

On pages 11 and 12, the Office Action rejects claims 2 and 3 under 35 U.S.C. § 103(a) as allegedly unpatentable over Matsui in view of Muratani, further in view of U.S. Patent No. 5,255,376 to Frank (hereinafter "Frank"). Applicant respectfully traverses this rejection.

Matsui and Muratani have been discussed above. Frank fails to remedy their deficiencies. In particular, Frank does not disclose a first request line connecting at least one encryption/decryption device to a control device and a second request line connecting a round key generator to a control device. While page 12 of the Office Action alleges that Frank discloses a bus [10] that contains a plurality of request

lines, Applicant respectfully submits that Frank's alleged teachings regarding request lines are inapplicable to the subject matter of independent claims 1 and 11. As disclosed in lines 42-50 of col. 6, for example, Frank's request lines are related to translation and slave cycles, involving a requesting device becoming a master device. Such a pattern is contrary to the current subject matter, in which both the encryption/decryption device and the round key generator must send requests to the control device.

Claims 2 and 3 depend from claim 1. Thus, claims 2 and 3 are allowable at least due to their respective dependencies from an allowable claim. Therefore, Applicant respectfully requests withdrawal of the rejection of claims 2 and 3 under 35 U.S.C. § 103(a).

3. Dependent Claims 5 and 14

On pages 12 and 13, the Office Action rejects claims 5 and 14 under 35 U.S.C. § 103(a) as allegedly unpatentable over Matsui in view of Muratani, further in view of U.S. Patent 5,919,251 to Tran (hereinafter "Tran"). Applicant respectfully traverses this rejection.

Matsui and Muratani have been discussed above. Tran fails to remedy their deficiencies. In particular, Tran only discloses a search mechanism for a rotating pointer buffer. As Tran lacks a control device coupled to both at least one

encryption/decryption device and a round key generator, Tran clearly lacks the first and second request lines recited in independent claims 1 and 11.

Claims 5 and 14 respectively depend from claims 1 and 11. Thus, claims 5 and 15 are allowable at least due to their respective dependencies from allowable claims. Therefore, Applicant respectfully requests withdrawal of the rejection of claims 5 and 14 under 35 U.S.C. § 103(a).

4. Dependent Claims 6, 7, 12, and 13

On pages 13-15, the Office Action rejects claims 6, 7, 12, and 13 under 35 U.S.C. § 103(a) as allegedly unpatentable over Matsui in view of Muratani, further in view of Hennessy. Applicant respectfully traverses this rejection.

Matsui and Muratani have been discussed above. Hennessy fails to remedy their deficiencies. In particular, Hennessy only describes connection of I/O devices to CPU/memory. Hennessy does not deal with separate round key generators and encryption/decryption devices, so Hennessy lacks the first and second request lines recited by independent claims 1 and 11.

Claims 6 and 7 depend from claim 1. Claims 12 and 13 depend from claim 11. Thus, claims 6, 7, 12, and 13 are allowable at least due to their respective dependencies from allowable claims. Therefore, Applicant respectfully requests withdrawal of the rejection of claims 6, 7, 12, and 13 under 35 U.S.C. § 103(a).

5. Dependent Claims 10 and 17

On pages 15-16, the Office Action rejects claims 10 and 17 under 35 U.S.C. § 103(a) as allegedly unpatentable over Matsui in view of Muratani, further in view of U.S. Patent Application No. 2003/0202658 to Verbauwhede (hereinafter "Verbauwhede"). Applicant respectfully traverses this rejection.

Matsui and Muratani have been discussed above. Verbauwhede fails to remedy their deficiencies. In particular, while Verbauwhede does provide an AES architecture, Verbauwhede teaches away from the first and second request lines recited in independent claims 1 and 11 by having an encryption module [Fig. 2: 10] directly coupled to a key scheduling module [12]. Thus, Verbauwhede clearly lacks a control device having separate request lines connected to at least one encryption/decryption device and a round key generator.

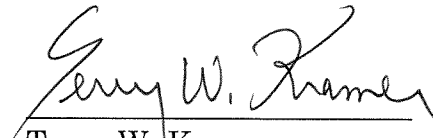
Claims 10 and 17 respectively depend from independent claims 1 and 11. Thus, claims 10 and 17 are allowable at least due to their respective dependencies from allowable claims. Therefore, Applicant respectfully requests withdrawal of the rejection of claims 10 and 17 under 35 U.S.C. § 103(a).

CONCLUSION

In view of the remarks above, Applicant believes that each of the rejections/objections has been overcome and the application is in condition for allowance. In the event that the fees submitted prove to be insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account. Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the attorney overseeing the application file, Aaron Waxler, of NXP Corporation at (408) 474-5029.

Respectfully submitted,
KRAMER & AMADO, P.C.

Date: June 8, 2009


Terry W. Kramer
Registration No.: 41,541

Please direct all correspondence to:
Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131
CUSTOMER NO.: 65913